



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/721,335	11/26/2003	Martin Soukup	57983.000166	8387
7590	07/09/2007		EXAMINER	
Thomas E. Anderson Hunton & Williams LLP 1900 K Street, N.W. Washington, DC 20006-1109			ZHU, BO HUI ALVIN	
			ART UNIT	PAPER NUMBER
			2616	
			MAIL DATE	
			07/09/2007	DELIVERY MODE
				PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

51

<b>Office Action Summary</b>	Application No.	Applicant(s)
	10/721,335	SOUKUP, MARTIN
	Examiner Bo Hui A. Zhu	Art Unit 2616

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

1) Responsive to communication(s) filed on 26 November 2003.  
 2a) This action is FINAL.                            2b) This action is non-final.  
 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

4) Claim(s) 1-21 is/are pending in the application.  
 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.  
 5) Claim(s) \_\_\_\_\_ is/are allowed.  
 6) Claim(s) 1-21 is/are rejected.  
 7) Claim(s) \_\_\_\_\_ is/are objected to.  
 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

9) The specification is objected to by the Examiner.  
 10) The drawing(s) filed on 26 November 2003 is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).  
 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. § 119

12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All    b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

#### Attachment(s)

1) Notice of References Cited (PTO-892)  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)  
 3) Information Disclosure Statement(s) (PTO/SB/08)  
 Paper No(s)/Mail Date \_\_\_\_\_.

4) Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_.  
 5) Notice of Informal Patent Application  
 6) Other: \_\_\_\_\_.

## DETAILED ACTION

### ***Claim Rejections - 35 USC § 101***

1. 35 U.S.C. 101 reads as follows:

Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

2. Claims 10 and 11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Regarding claim 10, a claim drawn to a “signal embodied in ... one carrier wave” does not constitute statutory subject matter such as a process, machine, article of manufacture or composition of matter.

Regarding claim 11, a claim drawn to a “processor readable carrier for storing a computer program of instructions” does not constitute statutory subject matter such as a process, machine, article of manufacture or composition of matter. In contrast, a claimed computer-readable medium encoded or embodied with a computer program product of code, or instructions, is a computer element which, when executed by a computer, defines structural and functional interrelationships between the instructions and the computer to permit the instructions functionality to be realized, and is thus statutory. Please see pages 30 and 53 of the Interim Guidelines for Examination of Patent Applications for Patent Subject Matter Eligibility

### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4. Claims 1 – 5, 9, 12 – 16 and 20 - 21 are rejected under 35 U.S.C. 102(a) as being anticipated by Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring".

(1) with regard to claims 1, 12 and 21:

Peng et al. disclose a method and system, comprising: identifying at least part of a source address of a packet; and determining whether the at least part of the source address matches at least one source address recorded within a predetermined time period prior to arrival of the packet (page 4, Section A and Fig. 3. The reference teaches matching the IP source address of the incoming packets to the source addresses recorded in a hash table for a time interval  $\Delta n$ ).

(2) with regard to claims 2 and 13:

Peng et al. further discloses the at least one source address is recorded in a hierarchical data structure (Fig. 3, the hash table records addresses in a hierarchical data structure).

(3) with regard to claims 3 and 14:

Peng et al. further discloses a Last Time Seen (LTS) value associated with each of the at least one source address is recorded (Fig. 3, the most recent time stamp).

(4) with regard to claim 4s and 15:

Peng et al. further discloses routing the packet if the at least part of the source address matches at least one source address recorded within the predetermined time period prior to the arrival of the packet; and recording an arrival time of the packet (page

4, Section A; the arrival time of the packet is recorded in the hash table, and the count for the number of packets having that address is updated).

(5) with regard to claims 5 and 16:

Peng et al. further discloses routing the packet with a warning if the at least part of the source address does not match at least one source address recorded within the predetermined time period prior to the arrival of the packet; and recording the at least part of the source address and an arrival time of the packet (page 4, Section A; if the address is not already in the hash table, it is added to it and the arrival time of the packet is recorded; the newly added address in the hash table can be viewed as a warning because the number of the newly added address appeared in a time slot is used to measured if a attack has occurred in the network).

(6) with regard to claims 9 and 20:

Peng et al. further discloses the source address of the packet is an internet protocol (IP) address (page 4, Section A).

### ***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. Claims 6 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring".

(1) with regard to claims 6 and 17:

Peng et al. does not disclose the warning is recorded in a read-only medium.

The Examiner takes Official Notice that the use of read-only medium is well known in the art. It is desirable to use read-only medium to store data because it provides higher security and protection to the data being stored since data stored in a read-only medium cannot be easily modified. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use read-only medium to store the warning in the system of Peng et al.

7. Claims 7, 8, 18 and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Lingafelt et al. (US 2002/0147925).

(1) with regard to claims 7 and 18:

Peng et al. further disclose issuing a warning if the at least part of the source address does not match at least one source address recorded within the predetermined time period prior to the arrival of the packet (page 4, Section A; if the address is not already in the hash table, it is added to it; the newly added address in the hash table can be viewed as a warning because the number of the newly added address appeared in a time slot is used to measured if a attack has occurred in the network).

Peng et al. however does not disclose discarding the packet.

Lingafelt et al. teaches discarding a packet if it does not match with an address in a database of addresses (335 in Fig. 3; paragraph [0025]).

It would have been desirable to discard the packet if it does not match an address in a database of addresses because it would improve the security of the system by not allowing unauthorized traffic to access network resources. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to discard the packets that are not authorized as taught by Lingafelt et al. in the system of Peng et al.

(2) with regard to claims 8 and 19:

Peng et al. does not disclose the warning is recorded in a read-only medium. The Examiner takes Official Notice that the use of read-only medium is well known in the art. It is desirable to use read-only medium to store data because it provides higher security and protection to the data being stored since data stored in a read-only medium cannot be easily modified. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to use read-only medium to store the warning in the system of Peng et al.

8. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Peng et al. "Detecting Distributed Denial of Service Attacks Using Source IP Address Monitoring" in view of Langberg et al. (US 5,852,630).

(1) with regard to claims 10 and 11:

Peng et al. discloses all of the subject matter as discussed in the rejection of claim 1. However, Peng et al. does not teach using a computer readable medium stored thereon a computer executable program for performing the method of claim 1.

Langberg et al. teaches a method for a transceiver warm start activation procedure can be implemented in software stored in a computer-readable medium. The computer-readable medium is an electronic, magnetic, optical, or other physical device or means that can contain or store a computer program for use by or in connection with a computer-related system or method (column 3, lines 51-65). Using a computer readable medium with program instruction code would be desirable because it would perform the same function of using hardware but offer the advantage of less expense, adaptability and flexibility. Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to include the limitation as taught by Langberg et al. into the system of Peng et al. so as to reduce cost and improve the adaptability and flexibility of the logic simulation.

### ***Conclusion***

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Bo Hui A. Zhu whose telephone number is (571)270-1086. The examiner can normally be reached on Mon-Thur 10am-6pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Hassan Kizou can be reached on (571)272-3088. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

BZ  
June 19, 2007



HASSAN KIZOU  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600